

THAT WHICH IS CLAIMED IS:

1. A cryptographic device comprising:
a cryptographic module and a communications module
removably coupled thereto;
said cryptographic module comprising
a first housing,
a user network interface carried by said
first housing,
a cryptographic processor carried by said
first housing and coupled to said user network
interface, and
a first connector carried by said first
housing and coupled to said cryptographic
processor;
said communications module comprising
a second housing,
a second connector carried by said second
housing and being removably mateable with said
first connector of said cryptographic module, and
a network communications interface carried by
said second housing and coupled to said second
connector.

2. The cryptographic device of Claim 1 wherein
said communications module comprises a predetermined one
from among a plurality of interchangeable communications
modules each for communicating over a different
communications media.

3. The cryptographic device of Claim 1 wherein said network communications interface comprises a wireless LAN (WLAN) communication circuit.

4. The cryptographic device of Claim 1 wherein said network communications interface comprises a wireline communication circuit.

5. The cryptographic device of Claim 1 wherein said network communications interface comprises a fiber optic communication circuit.

6. The cryptographic device of Claim 1 wherein said user network interface comprises an Ethernet LAN interface, and wherein said network interface comprises a network LAN interface.

7. The cryptographic device of Claim 1 further comprising a power circuit carried by said first housing and powering said cryptographic processor, said user network interface, and said communications module.

8. The cryptographic device of Claim 1 wherein said cryptographic processor implements an encryption algorithm to provide a predetermined security level.

9. The cryptographic device of Claim 1 wherein said cryptographic processor comprises:

a host network processor coupled to said user network interface; and

a cryptography circuit coupled to said host network processor.

10. The cryptographic device of Claim 9 wherein said cryptographic processor further comprises:

an encrypted data buffer circuit coupled between said user interface and said cryptography circuit; and

an unencrypted data buffer circuit coupled between said cryptography circuit and said network interface.

11. The cryptographic device of Claim 1 wherein said cryptographic module further comprises a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing.

12. The cryptographic device of Claim 11 wherein said tamper circuit comprises at least one conductor substantially surrounding said cryptographic processor, and wherein said cryptographic processor is disabled based upon a break in said at least one conductor.

13. A cryptographic device comprising:
a cryptographic module and a communications module removably coupled thereto;

said cryptographic module comprising

a first housing,

a user Local Area Network (LAN) interface carried by said first housing,

a cryptographic processor carried by said first housing and coupled to said user LAN interface,

a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing, and

a first connector carried by said first housing and coupled to said cryptographic processor;

said communications module comprising

a second housing,

a second connector carried by said second housing and being removably mateable with said first connector of said cryptographic module, and

a network LAN interface carried by said second housing and coupled to said second connector;

said communications module comprising a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media.

14. The cryptographic device of Claim 13 wherein said network LAN interface comprises a wireless LAN (WLAN) communication circuit.

15. The cryptographic device of Claim 13 wherein said network LAN interface comprises a wireline LAN communication circuit.

16. The cryptographic device of Claim 13 wherein said network LAN interface comprises a fiber optic LAN communication circuit.

17. The cryptographic device of Claim 13 wherein said user LAN interface comprises an Ethernet interface.

18. The cryptographic device of Claim 13 further comprising a power circuit carried by said first housing and powering said cryptographic processor, said user LAN interface, and said communications module.

19. The cryptographic device of Claim 13 wherein said cryptographic processor implements an encryption algorithm to provide a predetermined security level.

20. The cryptographic device of Claim 13 wherein said cryptographic processor comprises:

a host network processor coupled to said user LAN interface; and

a cryptography circuit coupled to said host network processor.

21. The cryptographic device of Claim 20 wherein said cryptographic processor further comprises:

an encrypted data buffer circuit coupled between said user LAN interface and said cryptography circuit; and

an unencrypted data buffer circuit coupled between said cryptography circuit and said network LAN interface.

22. The cryptographic device of Claim 13 wherein said tamper circuit comprises at least one conductor substantially surrounding said cryptographic processor, and wherein said cryptographic processor is disabled based upon a break in said at least one conductor.

23. A communications method comprising:

coupling a cryptographic module to a network device, the cryptographic module comprising a first housing, a user network interface carried by the first housing, a cryptographic processor carried by the first housing and coupled to the user network interface, and a first connector carried by the first housing and coupled to the cryptographic processor;

providing a communications module comprising a second housing, a second connector carried by the second housing, and a network communications interface carried by the second housing coupled to the second connector, the second connector of the communications module being removably mated with the first connector of the cryptographic module; and

using the network communications interface to communicate with a network.

24. The method of Claim 23 wherein the communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media.

25. The method of Claim 23 wherein the network communications interface comprises at least one of a wireless LAN (WLAN) communication circuit, a wireline communication circuit, and a fiber optic communication circuit.

26. The method of Claim 23 wherein the user network interface comprises an Ethernet LAN interface, and wherein the network communications interface comprises a network LAN interface.

27. A communications system comprising:
a plurality of network devices coupled together to define a network, and a cryptographic device coupled to at least one of said network devices;

said cryptographic device comprising a cryptographic module coupled to said at least one network device, and a communications module removably coupled to said cryptographic module;

said cryptographic module comprising

a first housing,

a user network interface carried by said first housing,

a cryptographic processor carried by said first housing and coupled to said user network interface, and

a first connector carried by said first housing and coupled to said cryptographic processor;

said communications module comprising

a second housing,

a second connector carried by said second housing and being removably mateable with said first connector of said cryptographic module, and

a network communications interface carried by said second housing and coupled to said second connector.

28. The communications system of Claim 27 wherein said communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media.

29. The communications system of Claim 27 wherein said network communications interface comprises at least one of a wireless LAN (WLAN) communication circuit, a wireline communication circuit, and a fiber optic communication circuit.

30. The communications system of Claim 27 wherein said user network interface comprises an Ethernet LAN interface, and wherein said network communications interface comprises a network LAN interface.

31. The communications system of Claim 27 further comprising a power circuit carried by said first housing and powering said cryptographic processor, said user network interface, and said communications module.

32. The communications system of Claim 27 wherein said cryptographic processor implements an encryption algorithm to provide a predetermined security level.

33. The communications system of Claim 27 wherein said cryptographic processor comprises:

a host network processor coupled to said user network interface; and

a cryptography circuit coupled to said host network processor.

34. The communications system of Claim 33 wherein said cryptographic processor further comprises:

an encrypted data buffer circuit coupled between said user network interface and said cryptography circuit; and

an unencrypted data buffer circuit coupled between said cryptography circuit and said network communications interface.

35. The communications system of Claim 27 wherein said cryptographic module further comprises a tamper circuit comprising at least one conductor substantially surrounding said cryptographic processor, and wherein said cryptographic processor is disabled based upon a break in said at least one conductor.